INDIANA OFFICE OF TECHNOLOGY

GOVERNOR MITCH DANIELS

Employee Registration/Deregistration

July 8

Access Control

- Improving security through better access control processes
- 2 new security practices
  - Strengthening passwords
  - Ensuring appropriate setup and disabling of accounts
  - Applied to all domains, starting with ISD-SHARED
- Drivers for change
  - Unacceptable results – we can and must do the job better
  - Technology enablers
  - PCI compliance (BMV)

End User Registration

- Practice 8.2.3
  - Registration in Active Directory
    - New user account registration form triggers a help desk ticket
    - Requires a PeopleSoft ID prior to activation, contractors as well
    - PeopleSoft can email Security Coordinators of a new employee if this aids the agencies internal processes
    - Agency can order "template" user rights
  - No additional work, timing changes
    - Concerns about getting new employees productive quickly
    - PeopleSoft does not allow for issuing a PeopleSoft ID in advance
  - Registration process is designed to improve deregistration

End User Deregistration

- Practice 8.2.3
  - Deregistration is initiated through on-line form that generates a help desk ticket
  - Includes agency instructions on where to place email and home folder information
  - Account disabled by IOT
  - Two safety nets
    - Auto-disable process upon termination keyed from PeopleSoft (PCI compliance requires immediate disable)
    - Any slipping through will be disabled at 90 day mark

Transfers of Employment

- Transfers to different teams will be treated similar to terminations
- Information is owned by the team
  - Includes files
  - Includes email
- Files and email can be provided to the employee by his/her former team
- Email addresses will be replicated when possible

Terminated end users

- Clean-up process goal – To eliminate active accounts for terminated staff
- The e-mailed spreadsheets require one of two actions:
  - Use web link to deregister user
  - Reply back with comments on status
- Weekly reports to measure progress – process completed by August 1

Terminated end users (cont.)

- Using the web link
  - Must be a security coordinator to use
  - Must use caution because security coordinators can disable other agency accounts
  - http://caa.iot.in.gov/Request/DeleteRequest.aspx

Addressing Service Accounts

- Service account clean-up goal – eliminate those no longer used, make identification of those remaining easier
- Email spreadsheet with update
  - Identify those needing to stay, define owner, describe service – IOT will update
  - Identify those ready for deletion – IOT will delete

Password Minimums

- Practice 8.2.1
  - Targeting August 12 to move to the following Active Directory password specifications:
    - Minimum password length: 8 characters
    - Password complexity: Systems should enforce complex passwords ensuring that passwords are made up of at least three of the following attributes: upper and lower case letters, numeric characters, embedded spaces or special characters.
    - Password history: 24 previous passwords unavailable for reuse
    - Minimum password age: 1 day
    - Maximum password age: 90 days
    - Account lockout duration: 15 minutes
    - Account lockout threshold: 15 attempts
    - Reset lockout account after: 15 minutes

Password Minimums (cont.)

- Practice 8.2.1
  - Expect some initial grumbling, it gets easier as you go
  - It is not an unreasonable job requirement
  - Guidance to remembering passwords
    - Rule #1 - Don't write it down
    - Rule #2 – If you're going to break rule #1, be very smart about it
    - Yellow sticky notes on monitors, laptops = discipline
    - http://www.in.gov/iot/2588.htm#Password_Management
  - Effective on next password change – not all at once
- Does not apply to service accounts

INDIANA OFFICE OF TECHNOLOGY

Access Control

- Questions